PHYSICAL AND PERSONNEL SECURITY INVESTIGATIONS

INTELLIGENCE CHARTER ISSUE PAPER FOR THE

SPECIAL COORDINATION COMMITTEE

I. Background: This paper describes in summary fashion current practices and procedures in the conduct of personnel and physical security investigations by the entities of the intelligence community and presents basic issues that require resolution by the Special Coordination Committee in order to develop intelligence charter provisions governing the collection of information that concerns United States persons for these purposes. The general issues in this area are:

a. Whether, and under what conditions, authority should be granted for unconsented collection of nonpublic information that concerns U.S. persons in the course of personnel security investigations;

b. Whether, and to what extent, should authority be granted for such collection in connection with maintaining the physical security of intelligence facilities, information, and personnel; and,

c. Whether, and subject to which limitations, should such collection be authorized in order to identify, investigate or prevent breaches of security rules, regulations and contractual obligations.

II. Current Practice: Executive Order 12036 currently authorizes CIA, DOD and NSA to protect the security of their installations, activities, information and personnel by "appropriate means" including "such investigations of applicants, employees, contractors, and other persons with similar associations" with those entities as are necessary. Current security investigative activities that concern U.S. persons may be loosely grouped under three general headings: (i) personnel security, (ii) physical security of facilities, information and personnel, and (iii) violations of security rules and regulations. These types of activities are all engaged in, to one degree or another, by CIA, DOD, FBI, State, and NSA.

(i) Personnel security investigations would include the collection of information concerning U.S. persons who are being considered for access to intelligence information or facilities and would include applicants for various forms

of staff or contract or proprietary employment or for clearances, sources or contacts who have agreed to assist the government, contractors, consultants, detailees, and service personnel (such as guards, painters, and telephone and other equipment maintenance personnel), and present employees, contractors, consultants, or other persons with current access to intelligence information to determine their continued suitability for such access. Background information would be collected concerning individuals in these categories through means and to a depth that would vary depending on the degree and scope of access to be granted. The minimum inquiry would consist of a request for review of entity, national agency, or local and municipal police records for any existing information concerning the subject, and the maximum inquiry would involve a "full field investigation" that could delve as much as 15 years into the subject's background and include, at least as to CIA employees and civilian employees of NSA, a polygraph interview. In addition, periodic reinvestigations of these types of persons, including a counterintelligence-oriented polygraph interview, could be scheduled as appropriate covering the intervening period since the last investigation. All such inquiries currently are conducted only with the consent of the invididual concerned, except for preliminary national agency records reviews that may be conducted by CIA solely to establish the identity of a potential source or contact. (The collection of information concerning potential sources is the subject of a separate issue paper.) Spouses of applicants for employment may be the subject of national agency records reviews, and the new spouse of a current employee may be the subject of a field investigation inquiry extending over the prior five years. Field investigations could include neighborhood inquiries, birth records, and police and, if appropriate, credit inquiries. In certain background inquiries conducted by CIA where cover considerations require, the subject, although providing biographic data and consenting, or the persons being interviewed, may not be ware that the subject of the inquiry will be working either for an intelligence entity or for an entity assisting the U.S. Government.

(ii) Physical security investigations encompass so-called "site suitability" reviews and threats to the integrity or safety of entity facilities, information, or personnel. Site suitability investigations entail preliminarily surveying the area surrounding the proposed location of an overt or clandestine intelligence activity and reviewing entity, and sometimes national agency, records to determine whether entities or persons in the immediate area pose a security problem for the activity. For example, it would not do to locate a CIA or FBI meeting site next door to a Soviet trade mission. Investigations relating to threats to facilities,

information, or personnel are tailored to the circumstances. Where a crowd or demonstration appears to pose a threat to an installation, the appropriate federal, state, military, or local police authorities are contacted and the intelligence entity representatives generally limit their activities to support of these police officials and to observing the crowd behavior at or near the facility. Suspicious activities by individuals outside entity facilities (for example, use of telephoto lens cameras or listing license plate numbers of cars entering or leaving) are also reported to the police, and the entity activity may be limited to obtaining a license plate number and attempting to identify the persons involved. Entity officials also would notify the FBI or Secret Service, as appropriate, of the contents of threatening mail or if the author of such mail should appear in the area. Where intrusion into an intelligence entity facility has occurred, the FBI, or local police if cover considerations require, would be notified and would investigate from a criminal or counterintelligence standpoint depending on the circumstances. Overseas, depending upon the circumstances, the local police may be contacted or the entity may conduct its own inquiry.

(iii) Breaches of security may be either inadvertent or deliberate. Inadvertent breaches by employees are usually discovered, investigated, and remedied administratively. Collection of information would proceed through interviews with the offending and other employees to determine the circumstances of the breach. Deliberate breaches of security regulations or suspected leaks by employees would be investigated by interviews with employees with knowledge of the situation. Executive Order 12036 requires that senior intelligence officials recommend to the Attorney General that serious or continuing security breaches be investigated by the FBI and where it is suspected that an employee may be furnishing information to a foreign entity, the matter would be turned over to the FBI.

III. Issues

1. Personnel Security. Executive Order 12036 authorizes the DCI to protect intelligence sources and methods, by lawful means, against disclosure by present CIA employees or contractors. It also authorizes investigations, as necessary, of applicants, employees, contractors, and other persons similarly associated with CIA, DOD, or NSA and permits by other than intrusive techniques the collection (using physical surveillance in some cases), retention, and dissemination of nonpublic information concerning U.S. persons without their consent when acquired in the course of "lawful" personnel security investigations or when related to present or former employees, present or former contractors or their employees, and applicants for such employment or

contracting when necessary to protect intelligence sources or methods. In limited circumstances this collection may include physical surveillance and pretext interviews.

S. 2525 would have authorized CIA to conduct "background investigations" (without elaboration but presumed to require consent) concerning applicants for employment, and would have authorized dissemination of information concerning the trustworthiness of any U.S. person who has, had, or is being considered for, access to classified information.

The issue is whether, and to what extent, statutory authority should be provided to collect nonpublic information that concerns U.S. persons without their consent in the context of personnel security investigations. It is assumed that any such authority for personnel security investigations need not extend to persons beyond present employees and their spouses to a limited degree, present contractors of various types and their employees, applicants for employment with an intelligence entity or proprietary and their spouses and close relatives to a limited degree, applicants for contractor status, and persons who are being considered for access to intelligence facilities or information. It is also assumed that such authority need not include use of electronic surveillance (or monitoring), physical searches (including mail opening), or mail covers. The techniques that remain for consideration include only nonpublic sources of information, physical surveillance, covert human source inquiries, pretext and third party interviews, and federal, state and local records reviews. The options then appear to include:

Option A - Provide no authority for collection of nonpublic information without consent;

Option B - Provide limited authority for such collection only to the extent consent is unavailable or impractical, and only as necessary to determine suitability or trustworthiness, and only through use of all or some of the available techniques;

Option C - Provide unlimited authority for such collection, or authority limited in some general way as to extent or technique, but subject to regulation by entity procedures approved by the Attorney General;

Option D - Provide unlimited authority, leaving regulation to entity heads.

2. Physical Security. Executive Order 12036 authorizes CIA, DOD and NSA to protect the security of their facilities, information, and personnel by "appropriate means". The Order also permits collection (using physical surveillance in some cases), retention, and dissemination of nonpublic information that concerns an unconsenting U.S. person arising out of "lawful" physical security investigations, or concerning present or former employees or contractors or their contacts, or concerning persons or activities that constitute a "clear threat" to any intelligence facility or personnel provided it is retained only by the threatened entity and the Secret Service and FBI if appropriate. The Order further exempts from its restrictions concerning relations with law enforcement authorities, cooperation with law enforcement entities to protect facilities and personnel.

S. 2525 would have authorized unconsented collection of information concerning any U.S. person in or near an intelligence facility to determine whether to exclude that person, but such collection would have been limited to physical surveillance, and requests for reviews of federal, state and local entities. In addition, S. 2525 would have authorized unconsented, nonpublic collection as to U.S. persons who are "reasonably believed to be engaging in any activity which poses a clear threat" to any intelligence facility or personnel, but such collection would have been limited to physical surveillance in the immediate vicinity of the facility, pretext interviews, and requests for reviews of federal, state and local entities.

Again the issue centers on whether and to what extent should authority be provided to collect nonpublic information that concerns U.S. persons without their consent in the context of physical security investigations. It is assumed here also that specialized authority to use electronic surveillance and monitoring, physical searches (including mail opening), or mail covers is unnecessary. This leaves open for discussion the use of such techniques as physical surveillance, nonpublic sources of information, covert human sources, pretext and third party interviews, and federal, state, and local records reviews. The options then appear to include:

Option A - Provide no authority for collection of nonpublic information without consent.

Option B - Provide limited authority for such collection only to the extent necessary to protect intelligence activities (e.g., site suitability investigations) or in the U.S. to determine whether to refer a matter (e.g., threats or disturbances) to law enforcement authorities, and only through use of all or some of the available techniques.

Option C - Provide unlimited authority for such collection, or authority limited in some general way as to extent or techniques, but subject to regulation by entity procedures approved by the Attorney General;

Option D - Provide unlimited authority, leaving regulation to entity heads.

3.- Breaches of Security. Executive Order 12036 places responsibility in the DCI to protect against disclosure of intelligence sources and methods by present or former CIA employees or contractors through "lawful means". Senior intelligence officials are charged by the Order with reporting serious or continuing security breaches to the Attorney General and recommending an FBI investigation. This provision was intended to focus responsibility for investigating security violations in the FBI and, to some extent, to compensate for the limitations imposed upon such activities by the intelligence entities. The Order also authorizes CIA, DOD and NSA to protect security by "appropriate means", including necessary investigations of applicants, employees, contractors, and other similarly associated persons. Physical surveillance is permitted by the Order for the purpose of protecting intelligence sources and methods so long as limited within the U.S., insofar as U.S. persons are concerned, to present employees, contractors and their employees, military personnel, and persons in contact with such persons, and outside the U.S. also to persons formerly in any of these categories. Collection, retention, and dissemination of nonpublic information concerning U.S. persons without their consent is permitted under the Order regarding present or former employees, contractors and their employees, and persons in contact with them, when necessary to protect sources and methods from disclosure.

S. 2525 would have provided authority to collect information concerning U.S. persons who are employees, or contractors and their employees to determine whether they have violated any security rule or regulation. Such collection would have required entity head approval to proceed beyond 180 days or to use covert human sources, mail covers, physical surveillance, or tax or other confidential records. In addition, S. 2525 would have provided authority to collect information concerning U.S. persons in contact with suspected intelligence agents, but limited to 90 days and only to identify the person and determine whether the person has, had, or will have access to sensitive information. In its November 1978 position paper, the SSCI indicated its preference that investigations of employees or former employees not be authorized unless there is "some evidence or reasonable probability" that the person has or is about to violate security regulations.

The issue here, as before, is focused on the nature and extent of the authority that should be granted in statute to collect nonpublic information and investigate actual or suspected breaches of security rules, regulations, or contractual obligations by U.S. persons without their consent, and the means by which such investigations should be carried out. Again it is assumed that electronic surveillance and monitoring or physical searches (including mail opening) will not be used for these purposes. It is also assumed that investigatory authority in this context need not extend beyond present and former employees and contractors and their employees, as well as, to a limited degree, persons with whom these individuals come into contact. The options appear to include:

Option A - Provide no authority for collection of nonpublic information without consent.

Option B - Provide unlimited authority for intelligence entities to collect nonpublic information concerning U.S. persons for these purposes, with or without a specific statutory standard.

Option C - Same as Option A but require entity procedures approved by the Attorney General.

Option D - Provide limited authority through such means as time limitations and restrictions on the use of certain techniques.

Option E - Provide limited authority to the intelligence entities but augment the responsibility and authority of the FBI to conduct such investigations on behalf of the intelligence entities.